

Entropy and Quantum Kolmogorov Complexity: A Quantum Brudno's Theorem

Fabio Benatti¹, Tyll Krüger^{2,3}, Markus Müller², Rainer Siegmund-Schultze², Arleta Szkoła²

¹ University of Trieste, Department of Theoretical Physics, Strada Costiera, 11, 34014 Trieste, Italy. E-mail: benatti@ts.infn.it

² Technische Universität Berlin, Fakultät II - Mathematik und Naturwissenschaften, Institut für Mathematik MA 7-2, Straße des 17. Juni 136, 10623 Berlin, Germany.
E-mail: {tkrueger, mueller, siegmund, szkola}@math.tu-berlin.de

³ Universität Bielefeld, Fakultät für Mathematik, Universitätsstr. 25, 33619 Bielefeld, Germany.

Received: 15 June 2005 / Accepted: 6 January 2006

Abstract: In classical information theory, entropy rate and algorithmic complexity per symbol are related by a theorem of Brudno. In this paper, we prove a quantum version of this theorem, connecting the von Neumann entropy rate and two notions of quantum Kolmogorov complexity, both based on the shortest qubit descriptions of qubit strings that, run by a universal quantum Turing machine, reproduce them as outputs.

1. Introduction

In recent years, the theoretical and experimental use of quantum systems to store, transmit and process information has spurred the study of how much of classical information theory can be extended to the new territory of quantum information and, vice versa, how much novel strategies and concepts are needed that have no classical counterpart.

We shall compare the relations between the rate at which entropy is produced by classical, respectively quantum, ergodic sources, and the complexity of the emitted strings of bits, respectively qubits.

According to Kolmogorov [24], the complexity of a bit string is the minimal length of a program for a Turing machine (*TM*) that produces the string. More in detail, the algorithmic complexity $K(\mathbf{i}^{(n)})$ of a string $\mathbf{i}^{(n)}$ is the length (counted in the number of bits) of the shortest program p that fed into a universal *TM* (*UTM*) \mathcal{U} yields the string as output, i.e. $\mathcal{U}(p) = \mathbf{i}^{(n)}$. For infinite sequences \mathbf{i} , in analogy with the entropy rate, one defines the *complexity rate* as $k(\mathbf{i}) := \lim_n \frac{1}{n} K(\mathbf{i}^{(n)})$, where $\mathbf{i}^{(n)}$ is the string consisting of the first n bits of \mathbf{i} , [2]. The universality of \mathcal{U} implies that changing the *UTM*, the difference in the complexity of a given string is bounded by a constant independent of the string; it follows that the complexity rate $k(\mathbf{i})$ is *UTM*-independent.

Different ways to quantify the complexity of qubit strings have been put forward; in this paper, we shall be concerned with some which directly generalize the classical definition by relating the complexity of qubit strings with their algorithmic description by means of quantum Turing machines (*QTM*).

For classical ergodic sources, an important theorem, proved by Brudno [10] and conjectured before by Zvonkin and Levin [43], establishes that the entropy rate equals the algorithmic complexity per symbol of almost all emitted bit strings. We shall show that this essentially also holds in quantum information theory.

For stationary classical information sources, the most important parameter is the *entropy rate* $h(\pi) = \lim_n \frac{1}{n} H(\pi^{(n)})$, where $H(\pi^{(n)})$ is the Shannon entropy of the ensembles of strings of length n that are emitted according to the probability distribution $\pi^{(n)}$. According to the Shannon-McMillan-Breiman theorem [6, 12], $h(\pi)$ represents the optimal compression rate at which the information provided by classical ergodic sources can be compressed and then retrieved with negligible probability of error (in the limit of longer and longer strings). Essentially, $nh(\pi)$ is the number of bits that are needed for reliable compression of bit strings of length n .

Intuitively, the less amount of patterns the emitted strings contain, the harder will be their compression, which is based on the presence of regularities and on the elimination of redundancies. From this point of view, the entropy rate measures the randomness of a classical source by means of its compressibility on the average, but does not address the randomness of single strings in the first instance. This latter problem was approached by Kolmogorov [24, 25], (and independently and almost at the same time by Chaitin [11], and Solomonoff [36]), in terms of the difficulty of their description by means of algorithms executed by universal Turing machines (*UTM*), see also [26].

On the whole, structureless strings offer no catch for writing down short programs that fed into a computer produce the given strings as outputs. The intuitive notion of random strings is thus mathematically characterized by Kolmogorov by the fact that, for large n , the shortest programs that reproduce them cannot do better than literal transcription [39].

Intuitively, one expects a connection between the randomness of single strings and the average randomness of ensembles of strings. In the classical case, this is exactly the content of a theorem of Brudno [10, 41, 22, 37] which states that for ergodic sources, the complexity rate of π -almost all infinite sequences \mathbf{i} coincides with the entropy rate, i.e. $k(\mathbf{i}) = h(\pi)$.

Quantum sources can be thought as black boxes emitting strings of qubits. The ensembles of emitted strings of length n are described by a density operator $\rho^{(n)}$ on the Hilbert spaces $(\mathbb{C}^2)^{\otimes n}$, which replaces the probability distribution $\pi^{(n)}$ from the classical case.

The simplest quantum sources are of Bernoulli type: they amount to infinite quantum spin chains described by shift-invariant states characterized by local density matrices $\rho^{(n)}$ over n sites with a tensor product structure $\rho^{(n)} = \rho^{\otimes n} := \bigotimes_{i=1}^n \rho$, where ρ is a density operator on \mathbb{C}^2 .

However, typical ergodic states of quantum spin-chains have richer structures that could be used as quantum sources: the local states $\rho^{(n)}$, not anymore tensor products, would describe emitted n -qubit strings which are correlated density matrices.

Similarly to classical information sources, quantum stationary sources (shift-invariant chains) are characterized by their entropy rate $s := \lim_n \frac{1}{n} S(\rho^{(n)})$, where $S(\rho^{(n)})$ denotes the von Neumann entropy of the density matrix $\rho^{(n)}$.

The quantum extension of the Shannon-McMillan Theorem was first obtained in [19] for Bernoulli sources, then a partial assertion was obtained for the restricted class of completely ergodic sources in [17], and finally in [7], a complete quantum extension was shown for general ergodic sources. The latter result is based on the construction of subspaces of dimension close to 2^{ns} , being typical for the source, in the sense that for sufficiently large block length n , their corresponding orthogonal projectors have an expectation value arbitrarily close to 1 with respect to the state of the quantum source. These typical subspaces have subsequently been used to construct compression protocols [9].

The concept of a universal quantum Turing machine (*UQTM*) as a precise mathematical model for quantum computation was first proposed by Deutsch [13]. The detailed construction of *UQTMs* can be found in [4, 1]: these machines work analogously to classical *TMs*, that is they consist of a read/write head, a set of internal control states and input/output tapes. However, the local transition functions among the machine's configurations (the programs or quantum algorithms) are given in terms of probability amplitudes, implying the possibility of linear superpositions of the machine's configurations. The quantum algorithms work reversibly. They correspond to unitary actions of the *UQTM* as a whole. An element of irreversibility appears only when the output tape information is extracted by tracing away the other degrees of freedom of the *UQTM*. This provides linear superpositions as well as mixtures of the output tape configurations consisting of the local states 0, 1 and blanks #, which are elements of the so-called *computational basis*. The reversibility of the *UQTM*'s time evolution is to be contrasted with recent models of quantum computation that are based on measurements on large entangled states, that is on irreversible processes, subsequently performed in accordance to the outcomes of the previous ones [32]. In this paper we shall be concerned with Bernstein-Vazirani-type *UQTMs* whose inputs and outputs may be bit or qubit strings [4].

Given the theoretical possibility of universal computing machines working in agreement with the quantum rules, it was a natural step to extend the problem of algorithmic descriptions as a complexity measure to the quantum case. Contrary to the classical case, where different formulations are equivalent, several inequivalent possibilities are available in the quantum setting. In the following, we shall use the definitions in [5] which, roughly speaking, say that the algorithmic complexity of a qubit string ρ is the logarithm in base 2 of the dimension of the smallest Hilbert space (spanned by computational basis vectors) containing a quantum state that, once fed into a *UQTM*, makes the *UQTM* compute the output ρ and halt.

In general, quantum states cannot be perfectly distinguished. Thus, it makes sense to allow some tolerance in the accuracy of the machine's output. As explained below, there are two natural ways to deal with this, leading to two (closely related) different complexity notions $QC^{\searrow 0}$ and QC^δ , which correspond to asymptotically vanishing, respectively small but fixed tolerance.

Both quantum algorithmic complexities $QC^{\searrow 0}$ and QC^δ are thus measured in terms of the length of *quantum* descriptions of qubit strings, in contrast to another definition [40] which defines the complexity of a qubit string as the length

of its shortest *classical* description. A third definition [15] is instead based on an extension of the classical notion of universal probability to that of universal density matrices. The study of the relations among these proposals is still in a very preliminary stage. For an approach to quantum complexity based on the amount of resources (quantum gates) needed to implement a quantum circuit reproducing a given qubit string see [27, 28].¹

The main result of this work is the proof of a weaker form of Brudno's theorem, connecting the quantum entropy rate s and the quantum algorithmic complexities $QC^{\setminus 0}$ and QC^δ of pure states emitted by quantum ergodic sources. It will be proved that there are sequences of typical subspaces of $(\mathbb{C}^2)^{\otimes n}$, such that the complexity rates $\frac{1}{n}QC^{\setminus 0}(q)$ and $\frac{1}{n}QC^\delta(q)$ of any of their pure-state projectors q can be made as close to the entropy rate s as one wants by choosing n large enough, and there are no such sequences with a smaller expected complexity rate.

The paper is divided as follows. In Section 2, a short review of the C^* -algebraic approach to quantum sources is given, while Section 3 states as our main result a quantum version of Brudno's theorem. In Section 4, a detailed survey of *QTM*s and of the notion of *quantum Kolmogorov complexity* is presented. In Section 5, based on a quantum counting argument, a lower bound is given for the quantum Kolmogorov complexity per qubit, while an upper bound is obtained in Section 5 by explicit construction of a short quantum algorithm able to reproduce any pure state projector q belonging to a particular sequence of high probability subspaces.

2. Ergodic Quantum Sources

In order to formulate our main result rigorously, we start with a brief introduction to the relevant concepts of the formalism of quasi-local C^* -algebras which is the most suited one for dealing with quantum spin chains. At the same time, we shall fix the notations.

We shall consider the lattice \mathbb{Z} and assign to each site $x \in \mathbb{Z}$ a C^* -algebra \mathcal{A}_x being a copy of a fixed finite-dimensional algebra \mathcal{A} , in the sense that there exists a $*$ -isomorphism $i_x : \mathcal{A} \rightarrow \mathcal{A}_x$. To simplify notations, we write $a \in \mathcal{A}_x$ for $i_x(a) \in \mathcal{A}_x$ and $a \in \mathcal{A}$. The algebra of observables associated to a finite $\Lambda \subset \mathbb{Z}$ is defined by $\mathcal{A}_\Lambda := \bigotimes_{x \in \Lambda} \mathcal{A}_x$. Observe that for $\Lambda \subset \Lambda'$ we have $\mathcal{A}_{\Lambda'} = \mathcal{A}_\Lambda \otimes \mathcal{A}_{\Lambda' \setminus \Lambda}$ and there is a canonical embedding of \mathcal{A}_Λ into $\mathcal{A}_{\Lambda'}$ given by $a \mapsto a \otimes \mathbf{1}_{\Lambda' \setminus \Lambda}$, where $a \in \mathcal{A}_\Lambda$ and $\mathbf{1}_{\Lambda' \setminus \Lambda}$ denotes the identity of $\mathcal{A}_{\Lambda' \setminus \Lambda}$. The infinite-dimensional quasi-local C^* -algebra \mathcal{A}^∞ is the norm completion of the normed algebra $\bigcup_{\Lambda \subset \mathbb{Z}} \mathcal{A}_\Lambda$, where the union is taken over all finite subsets Λ .

In the present paper, we mainly deal with qubits, which are the quantum counterpart of classical bits. Thus, in the following, we restrict our considerations to the case where \mathcal{A} is the algebra of observables of a qubit, i.e. the algebra $\mathcal{M}_2(\mathbb{C})$ of 2×2 matrices acting on \mathbb{C}^2 . Since every finite-dimensional unital C^* -Algebra \mathcal{A} is $*$ -isomorphic to a subalgebra of $\mathcal{M}_2(\mathbb{C})^{\otimes D}$ for some $D \in \mathbb{N}$, our results contain the general case of arbitrary \mathcal{A} . Moreover, the case of classical bits is covered by \mathcal{A} being the subalgebra of $\mathcal{M}_2(\mathbb{C})$ consisting of diagonal matrices only.

¹ Other considerations concerning quantum complexity can be found in [38] and [35].

Similarly, we think of \mathcal{A}_A as the algebra of observables of qubit strings of length $|A|$, namely the algebra $\mathcal{M}_{2^{|A|}}(\mathbb{C}) = \mathcal{M}_2(\mathbb{C})^{\otimes |A|}$ of $2^{|A|} \times 2^{|A|}$ matrices acting on the Hilbert space $\mathcal{H}_A := (\mathbb{C}^2)^{\otimes |A|}$. The quasi-local algebra \mathcal{A}^∞ corresponds to the doubly-infinite qubit strings.

The (right) shift τ is a $*$ -automorphism on \mathcal{A}^∞ uniquely defined by its action on local observables

$$\tau : a \in \mathcal{A}_{[m,n]} \mapsto a \in \mathcal{A}_{[m+1,n+1]} \quad (1)$$

where $[m, n] \subset \mathbb{Z}$ is an integer interval.

A state Ψ on \mathcal{A}^∞ is a normalized positive linear functional on \mathcal{A}^∞ . Each local state $\Psi_A := \Psi \upharpoonright \mathcal{A}_A$, $A \subset \mathbb{Z}$ finite, corresponds to a density operator $\rho_A \in \mathcal{A}_A$ by the relation $\Psi_A(a) = \text{Tr}(\rho_A a)$, for all $a \in \mathcal{A}_A$, where Tr is the trace on $(\mathbb{C}^2)^{\otimes |A|}$. The density operator ρ_A is a positive matrix acting on the Hilbert space \mathcal{H}_A associated with \mathcal{A}_A satisfying the normalization condition $\text{Tr} \rho_A = 1$. The simplest ρ_A correspond to one-dimensional projectors $P := |\psi_A\rangle\langle\psi_A|$ onto vectors $|\psi_A\rangle \in \mathcal{H}_A$ and are called pure states, while general density operators are linear convex combinations of one-dimensional projectors: $\rho_A = \sum_i \lambda_i |\psi_A^i\rangle\langle\psi_A^i|$, $\lambda_i \geq 0$, $\sum_j \lambda_j = 1$. We denote by $\mathcal{T}_1^+(\mathcal{H})$ the convex set of density operators acting on a (possibly infinite-dimensional) Hilbert space \mathcal{H} , whence $\rho_A \in \mathcal{T}_1^+(\mathcal{H}_A)$.

A state Ψ on \mathcal{A}^∞ corresponds one-to-one to a family of density operators $\rho_A \in \mathcal{A}_A$, $A \subset \mathbb{Z}$ finite, fulfilling the consistency condition $\rho_A = \text{Tr}_{A' \setminus A}(\rho_{A'})$ for $A \subset A'$, where Tr_A denotes the partial trace over the local algebra \mathcal{A}_A which is computed with respect to any orthonormal basis in the associated Hilbert space \mathcal{H}_A . Notice that a state Ψ with $\Psi \circ T = \Psi$, i.e. a shift-invariant state, is uniquely determined by a consistent sequence of density operators $\rho^{(n)} := \rho_{A(n)}$ in $\mathcal{A}^{(n)} := \mathcal{A}_{A(n)}$ corresponding to the local states $\Psi^{(n)} := \Psi_{A(n)}$, where $A(n)$ denotes the integer interval $[1, n] \subset \mathbb{Z}$, for each $n \in \mathbb{N}$.

As motivated in the introduction, in the information-theoretical context, we interpret the tuple $(\mathcal{A}^\infty, \Psi)$ describing the quantum spin chain as a stationary quantum source.

The von Neumann entropy of a density matrix ρ is $S(\rho) := -\text{Tr}(\rho \log \rho)$. By the subadditivity of S for a shift-invariant state Ψ on \mathcal{A}^∞ , the following limit, the quantum entropy rate, exists

$$s(\Psi) := \lim_{n \rightarrow \infty} \frac{1}{n} S(\rho^{(n)}) .$$

The set of shift-invariant states on \mathcal{A}^∞ is convex and compact in the weak*-topology. The extremal points of this set are called ergodic states: they are those states which cannot be decomposed into linear convex combinations of other shift-invariant states. Notice that in particular the shift-invariant product states defined by a sequence of density matrices $\rho^{(n)} = \rho^{\otimes n}$, $n \in \mathbb{N}$, where ρ is a fixed 2×2 density matrix, are ergodic. They are the quantum counterparts of Bernoulli (i.i.d.) processes. Most of the results in quantum information theory concern such sources, but, as mentioned in the introduction, more general ergodic quantum sources allowing correlations can be considered.

More concretely, the typical quantum source that has first been considered was a finite-dimensional quantum system emitting vector states $|v_i\rangle \in \mathbb{C}^2$ with probabilities $p(i)$. The state of such a source is the density matrix $\rho =$

$\sum_i p(i) |v_i\rangle\langle v_i|$ being an element of the full matrix algebra $\mathcal{M}_2(\mathbb{C})$; furthermore, the most natural source of qubit strings of length n is the one that emits vectors $|v_i\rangle$ independently one after the other at each stroke of time.² The corresponding state after n emissions is thus the tensor product

$$\rho^{\otimes n} = \sum_{i_1 i_2 \dots i_n} p(i_1) p(i_2) \dots p(i_n) |v_{i_1} \otimes v_{i_2} \otimes \dots \otimes v_{i_n}\rangle \langle v_{i_1} \otimes v_{i_2} \otimes \dots \otimes v_{i_n}|.$$

In the following, we shall deal with the more general case of *ergodic* sources defined above, which naturally appear e.g. in statistical mechanics (compare 1D spin chains with finite-range interaction).

When restricted to act only on n successive chain sites, namely on the local algebra $\mathcal{A}^{(n)} = \mathcal{M}_{2^n}(\mathbb{C})$, these states correspond to density matrices $\rho^{(n)}$ acting on $(\mathbb{C}^2)^{\otimes n}$ which are not simply tensor products, but may contain classical correlations and entanglement. The qubit strings of length n emitted by these sources are generic density matrices σ acting on $(\mathbb{C}^2)^{\otimes n}$, which are compatible with the state of the source Ψ in the sense that $\text{supp } \sigma \leq \text{supp } \rho^{(n)}$, where $\text{supp } \sigma$ denotes the support projector of the operator σ , that is the orthogonal projection onto the subspace where σ cannot vanish. More concretely, $\rho^{(n)}$ can be decomposed in uncountably many different ways into convex decompositions $\rho^{(n)} = \sum_i \lambda_i \sigma_i^{(n)}$ in terms of other density matrices $\sigma_i^{(n)}$ on the local algebra $\mathcal{A}^{(n)}$ each one of which describes a possible qubit string of length n emitted by the source.

3. Main Theorem

It turns out that the rates of the complexities $QC^{\searrow 0}$ (approximation-scheme complexity) and QC^δ (finite-accuracy complexity) of the typical pure states of qubit strings generated by an ergodic quantum source $(\mathcal{A}^\infty, \Psi)$ are asymptotically equal to the entropy rate $s(\Psi)$ of the source. A precise formulation of this result is the content of the following theorem. It can be seen as a quantum extension of Brudno's theorem as a convergence in probability statement, while the original formulation of Brudno's result is an almost sure statement.

We remark that a proper introduction to the concept of quantum Kolmogorov complexity needs some further considerations. We postpone this task to the next section.

In the remainder of this paper, we call a sequence of projectors $p_n \in \mathcal{A}^{(n)}$, $n \in \mathbb{N}$, satisfying $\lim_{n \rightarrow \infty} \Psi^{(n)}(p_n) = 1$ a *sequence of Ψ -typical projectors*.

Theorem 1 (Quantum Brudno Theorem).

Let $(\mathcal{A}^\infty, \Psi)$ be an ergodic quantum source with entropy rate s . For every $\delta > 0$, there exists a sequence of Ψ -typical projectors $q_n(\delta) \in \mathcal{A}^{(n)}$, $n \in \mathbb{N}$, i.e. $\lim_{n \rightarrow \infty} \Psi^{(n)}(q_n(\delta)) = 1$, such that for n large enough every one-dimensional projector $q \leq q_n(\delta)$ satisfies

$$\frac{1}{n} QC^{\searrow 0}(q) \in (s - \delta, s + \delta), \quad (2)$$

$$\frac{1}{n} QC^\delta(q) \in (s - \delta(2 + \delta), s + \delta). \quad (3)$$

² Here we use Dirac's bra-ket notation, where a bra $\langle v|$ is a vector in a Hilbert space and a ket $|v\rangle$ is its dual vector.

Moreover, s is the optimal expected asymptotic complexity rate, in the sense that every sequence of projectors $q_n \in \mathcal{A}^{(n)}$, $n \in \mathbb{N}$, that for large n may be represented as a sum of mutually orthogonal one-dimensional projectors that all violate the lower bounds in (2) and (3) for some $\delta > 0$, has an asymptotically vanishing expectation value with respect to Ψ .

4. QTMs and Quantum Kolmogorov Complexity

Algorithmic complexity measures the degree of randomness of a single object. It is defined as the minimal description length of the object, relative to a certain "machine" (classically a *UTM*). In order to properly introduce a quantum counterpart of Kolmogorov complexity, we thus have to specify what kind of objects we want to describe (outputs), what the descriptions (inputs) are made of, and what kind of machines run the algorithms.

In accordance to the introduction, we stipulate that inputs and outputs are so-called (pure or mixed) *variable-length qubit strings*, while the reference machines will be *QTMs* as defined by Bernstein and Vazirani [4], in particular universal *QTMs*.

4.1. Variable-Length Qubit Strings. Let $\mathcal{H}_k := (\mathbb{C}^{\{0,1\}})^{\otimes k}$ be the Hilbert space of k Qubits ($k \in \mathbb{N}_0$). We write $\mathbb{C}^{\{0,1\}}$ for \mathbb{C}^2 to indicate that we fix two orthonormal *computational basis vectors* $|0\rangle$ and $|1\rangle$. Since we want to allow superpositions of different lengths k , we consider the Hilbert space $\mathcal{H}_{\{0,1\}^*}$ defined as

$$\mathcal{H}_{\{0,1\}^*} := \bigoplus_{k=0}^{\infty} \mathcal{H}_k .$$

The classical finite binary strings $\{0,1\}^*$ are identified with the computational basis vectors in $\mathcal{H}_{\{0,1\}^*}$, i.e. $\mathcal{H}_{\{0,1\}^*} \simeq \ell^2(\{\lambda, 0, 1, 00, 01, \dots\})$, where λ denotes the empty string. We also use the notation

$$\mathcal{H}_{\leq n} := \bigoplus_{k=0}^n \mathcal{H}_k$$

and treat it as a subspace of $\mathcal{H}_{\{0,1\}^*}$. A (variable-length) *qubit string* $\sigma \in \mathcal{T}_1^+(\mathcal{H}_{\{0,1\}^*})$ is a density operator on $\mathcal{H}_{\{0,1\}^*}$. We define the *length* $\ell(\sigma) \in \mathbb{N}_0 \cup \{\infty\}$ of a qubit string $\sigma \in \mathcal{T}_1^+(\mathcal{H}_{\{0,1\}^*})$ as

$$\ell(\sigma) := \min\{n \in \mathbb{N}_0 \mid \sigma \in \mathcal{T}_1^+(\mathcal{H}_{\leq n})\} \quad (4)$$

or as $\ell(\sigma) = \infty$ if this set is empty (this will never occur in the following).

There are two reasons for considering variable-length and also mixed qubit strings. First, we want our result to be as general as possible. Second, a *QTM* will naturally produce superpositions of qubit strings of different lengths; mixed outputs appear naturally while tracing out the other parts of the *QTM* (input tape, control, head) after halting.

In contrast to the classical situation, there are uncountably many qubit strings that cannot be perfectly distinguished by means of any quantum measurement. If

$\rho, \sigma \in \mathcal{T}_1^+(\mathcal{H}_{\{0,1\}^*})$ are two qubit strings with finite length, then we can quantify their distance in terms of the trace distance

$$\|\rho - \sigma\|_{\text{Tr}} := \frac{1}{2} \text{Tr} |\rho - \sigma| = \frac{1}{2} \sum_i |\lambda_i|, \quad (5)$$

where the λ_i are the eigenvalues of the Hermitian operator $|\rho - \sigma| := \sqrt{(\rho - \sigma)^*(\rho - \sigma)}$.

In Subsection 4.3, we will define Quantum Kolmogorov Complexity $QC(\rho)$ for qubit strings ρ . Due to the considerations above, it cannot be expected that the qubit strings ρ are reproduced exactly, but it rather makes sense to demand the strings to be generated within some trace distance δ . Another possibility is to consider "approximation schemes", i.e. to have some parameter $k \in \mathbb{N}$, and to demand the machine to approximate the desired state better and better the larger k gets. We will pursue both approaches, corresponding to equations (9) and (10) below.

Note that we can identify every density operator $\rho \in \mathcal{A}^{(n)}$ on the local n -block algebra with its corresponding qubit string $\tilde{\rho} \in \mathcal{T}_1^+(\mathcal{H}_n) \subset \mathcal{T}_1^+(\mathcal{H}_{\{0,1\}^*})$ such that $\ell(\tilde{\rho}) = n$. Similarly, we identify qubit strings $\sigma \in \mathcal{T}_1^+(\mathcal{H}_{\{0,1\}^*})$ of finite length ℓ with the state of the input or output tape of a *QTM* (see Subsection 4.2) containing the state in the cell interval $[0, \ell - 1]$ and vice versa.

4.2. Mathematical Description of QTMs. Due to the equivalence of various models for quantum computation, the definition of Quantum Kolmogorov Complexity should be rather insensitive to the details of the underlying machine. Nevertheless, there are some details which are relevant for our theorem. Thus, we have to give a thorough definition of what we mean by a *QTM*.

Bernstein and Vazirani ([4], Def. 3.2.2) define a quantum Turing machine M as a triplet (Σ, Q, δ) , where Σ is a finite alphabet with an identified blank symbol $\#$, and Q is a finite set of states with an identified initial state q_0 and final state $q_f \neq q_0$. The function $\delta : Q \times \Sigma \rightarrow \tilde{\mathbb{C}}^{\Sigma \times Q \times \{L, R\}}$ is called the *quantum transition function*. The symbol $\tilde{\mathbb{C}}$ denotes the set of complex numbers $\alpha \in \mathbb{C}$ such that there is a deterministic algorithm that computes the real and imaginary parts of α to within 2^{-n} in time polynomial in n .

One can think of a *QTM* as consisting of a two-way infinite tape \mathbf{T} of cells indexed by \mathbb{Z} , a control \mathbf{C} , and a single "read/write" head \mathbf{H} that moves along the tape. A (classical) configuration is a triplet $((\sigma_i)_{i \in \mathbb{Z}}, q, k) \in \Sigma^{\mathbb{Z}} \times Q \times \mathbb{Z}$ such that only a finite number of tape cell contents σ_i are non-blank (q and k are the state of the control and the position of the head respectively). Let C be the set of all configurations, and define the Hilbert space $\mathcal{H}_{QTM} := \ell^2(C)$, which can be written as $\mathcal{H}_{QTM} = \mathcal{H}_{\mathbf{C}} \otimes \mathcal{H}_{\mathbf{H}} \otimes \mathcal{H}_{\mathbf{T}}$.

The transition function δ generates a linear operator U_M on \mathcal{H}_{QTM} describing the time evolution of the *QTM*. We identify $\sigma \in \mathcal{T}_1^+(\mathcal{H}_{\{0,1\}^*})$ with the initial state of M on input σ , which is according to the definition in [4] a state on \mathcal{H}_{QTM} where σ is written on the input track over the cell interval $[0, l(\sigma) - 1]$, the empty state $\#$ is written on the remaining cells of the input track and on the whole output track, the control is in the initial state q_0 and the head is in position 0. Then, the state $M^t(\sigma)$ of M on input σ at time $t \in \mathbb{N}_0$ is given by

$M^t(\sigma) = (U_M)^t \sigma (U_M^*)^t$. The state of the control at time t is thus given by partial trace over all the other parts of the machine, that is $M_{\mathbf{C}}^t(\sigma) := \text{Tr}_{\mathbf{H}, \mathbf{T}}(M^t(\sigma))$. In accordance with [4], Def. 3.5.1, we say that the QTM M *halts at time* $t \in \mathbb{N}_0$ *on input* $\sigma \in \mathcal{T}_1^+(\mathcal{H}_{\{0,1\}^*})$, if and only if

$$\langle q_f | M_{\mathbf{C}}^t(\sigma) | q_f \rangle = 1 \quad \text{and} \quad \langle q_f | M_{\mathbf{C}}^{t'}(\sigma) | q_f \rangle = 0 \quad \text{for every } t' < t, \quad (6)$$

where $q_f \in Q$ is the special state of the control (specified in the definition of M) signalling the halting of the computation.

Denote by $\tilde{\mathcal{H}}(t) \subset \mathcal{H}_{\{0,1\}^*}$ the set of vector inputs with equal halting time t . Observe that the above definition implies that $\mathcal{H}(t) := \{c |\phi\rangle : c \in \mathbb{C}, |\phi\rangle \in \tilde{\mathcal{H}}(t)\}$ is equal to the linear span of $\tilde{\mathcal{H}}(t)$, i.e. $\mathcal{H}(t)$ is a linear subspace of $\mathcal{H}_{\{0,1\}^*}$. Moreover for $t \neq t'$ the corresponding subspaces $\mathcal{H}(t)$ and $\mathcal{H}(t')$ are mutually orthogonal, because otherwise one could perfectly distinguish non-orthogonal vectors by means of the halting time. It follows that the subset of $\mathcal{T}_1^+(\mathcal{H}_{\{0,1\}^*})$ on which a QTM M halts is a union $\bigcup_{t \in \mathbb{N}} \mathcal{T}_1^+(\mathcal{H}(t))$.

For our purpose, it is useful to consider a special class of QTMs with the property that their tape \mathbf{T} consists of two different tracks, an *input track* \mathbf{I} and an *output track* \mathbf{O} . This can be achieved by having an alphabet which is a Cartesian product of two alphabets, in our case $\Sigma = \{0, 1, \#\} \times \{0, 1, \#\}$. Then, the tape Hilbert space $\mathcal{H}_{\mathbf{T}}$ can be written as $\mathcal{H}_{\mathbf{T}} = \mathcal{H}_{\mathbf{I}} \otimes \mathcal{H}_{\mathbf{O}}$.

Definition 1 (Quantum Turing Machine (QTM)).

A partial map $M : \mathcal{T}_1^+(\mathcal{H}_{\{0,1\}^*}) \rightarrow \mathcal{T}_1^+(\mathcal{H}_{\{0,1\}^*})$ will be called a QTM, if there is a Bernstein-Vazirani two-track QTM $\tilde{M} = (\Sigma, Q, \delta)$ (see [4], Def. 3.5.5) with the following properties:

- $\Sigma = \{0, 1, \#\} \times \{0, 1, \#\}$,
- the corresponding time evolution operator $U_{\tilde{M}}$ is unitary,
- if \tilde{M} halts on input σ with a variable-length qubit string $\rho \in \mathcal{T}_1^+(\mathcal{H}_{\{0,1\}^*})$ on the output track starting in cell 0 such that the i -th cell is empty for every $i \notin [0, \ell(\rho) - 1]$, then $M(\sigma) = \rho$; otherwise, $M(\sigma)$ is undefined.

In general, different inputs σ have different halting times t and the corresponding outputs are essentially results of different unitary transformations given by U_M^t . However, as the subset of $\mathcal{T}_1^+(\mathcal{H}_{\{0,1\}^*})$ on which M is defined is of the form $\bigcup_{t \in \mathbb{N}} \mathcal{T}_1^+(\mathcal{H}(t))$, the action of the partial map M on this subset may be extended to a valid quantum operation³ on $\mathcal{T}(\mathcal{H}_{\{0,1\}^*})$:

Lemma 1 (QTMs are Quantum Operations).

For every QTM M there is a quantum operation $\mathcal{M} : \mathcal{T}(\mathcal{H}_{\{0,1\}^*}) \rightarrow \mathcal{T}(\mathcal{H}_{\{0,1\}^*})$, such that for every $\sigma \in \bigcup_{t \in \mathbb{N}} \mathcal{T}_1^+(\mathcal{H}(t))$

$$M(\sigma) = \mathcal{M}(\sigma).$$

Proof. Let \mathcal{B}_t and \mathcal{B}_{\perp} be an orthonormal basis of $\mathcal{H}(t)$, $t \in \mathbb{N}$, and the orthogonal complement of $\bigoplus_{t \in \mathbb{N}} \mathcal{H}(t)$ within $\mathcal{H}_{\{0,1\}^*}$, respectively. We add an ancilla Hilbert space $\mathcal{H}_{\mathbf{A}} := \ell^2(\mathbb{N}_0)$ to the QTM, and define a linear operator

³ Recall that quantum operations are trace-preserving completely positive maps on the trace-class operators $\mathcal{T}(\mathcal{H})$ on the system Hilbert space \mathcal{H} , see [18].

$V_M : \mathcal{H}_{\{0,1\}^*} \rightarrow \mathcal{H}_{QTM} \otimes \mathcal{H}_A$ by specifying its action on the orthonormal basis vectors $\cup_{t \in \mathbb{N}} \mathcal{B}_t \cup \mathcal{B}_\perp$:

$$V_M |b\rangle := \begin{cases} (U_M^t |b\rangle) \otimes |t\rangle & \text{if } |b\rangle \in \mathcal{B}_t, \\ |b\rangle \otimes |0\rangle & \text{if } |b\rangle \in \mathcal{B}_\perp. \end{cases} \quad (7)$$

Since the right hand side of (7) is a set of orthonormal vectors in $\mathcal{H}_{QTM} \otimes \mathcal{H}_A$, the map V_M is a partial isometry. Thus, the map $\sigma \mapsto V_M \sigma V_M^*$ is trace-preserving, completely positive ([31]). Its composition with the partial trace, given by $\mathcal{M}(\sigma) := \text{Tr}_{\mathbf{C}, \mathbf{H}, \mathbf{I}, \mathbf{A}}(V_M \sigma V_M^*)$, is a quantum operation. \square

4.3. Quantum Algorithmic Complexity. The typical case we want to study is the (approximate) reproduction of a density matrix $\rho \in \mathcal{T}_1^+(\mathcal{A}^{(n)})$ by a QTM M . This means that there is a "quantum program" $\sigma \in \mathcal{T}_1^+(\mathcal{H}_{\{0,1\}^*})$, such that $M(\sigma) \approx \rho$ in a sense explained below.

We are particularly interested in the case that the program σ is shorter than ρ itself, i.e. that $\ell(\sigma) < \ell(\rho)$. On the whole, the minimum possible length $\ell(\sigma)$ for ρ will be defined as the *quantum algorithmic complexity* of ρ .

As already mentioned, there are at least two natural possible definitions. The first one is to demand only approximate reproduction of ρ within some trace distance δ . The second one is based on the notion of an approximation scheme. To define the latter, we have to specify what we mean by supplying a QTM with *two* inputs, the qubit string and a parameter:

Definition 2 (Parameter Encoding).

Let $k \in \mathbb{N}$ and $\sigma \in \mathcal{T}_1^+(\mathcal{H}_{\{0,1\}^*})$. We define an encoding $\mathcal{C} : \mathbb{N} \times \mathcal{T}_1^+(\mathcal{H}_{\{0,1\}^*}) \rightarrow \mathcal{T}_1^+(\mathcal{H}_{\{0,1\}^*})$ of a pair (k, σ) into a single string $\mathcal{C}(k, \sigma)$ by

$$\mathcal{C}(k, \sigma) := |\tilde{k}\rangle\langle\tilde{k}| \otimes \sigma,$$

where \tilde{k} denotes the (classical) string consisting of $\lfloor \log k \rfloor$ 1's, followed by one 0, followed by the $\lfloor \log k \rfloor + 1$ binary digits of k , and $|\tilde{k}\rangle\langle\tilde{k}|$ is the corresponding projector in the computational basis⁴. For every QTM M , we set

$$M(k, \sigma) := M(\mathcal{C}(k, \sigma)).$$

Note that

$$\ell(\mathcal{C}(k, \sigma)) = 2\lfloor \log k \rfloor + 2 + \ell(\sigma). \quad (8)$$

The QTM M has to be constructed in such a way that it is able to decode both k and σ from $\mathcal{C}(k, \sigma)$, which is an easy classical task.

Definition 3 (Quantum Algorithmic Complexity).

Let M be a QTM and $\rho \in \mathcal{T}_1^+(\mathcal{H}_{\{0,1\}^*})$ a qubit string. For every $\delta \geq 0$, we define the finite-accuracy quantum complexity $QC_M^\delta(\rho)$ as the minimal length $\ell(\sigma)$ of any quantum program $\sigma \in \mathcal{T}_1^+(\mathcal{H}_{\{0,1\}^*})$ such that the corresponding output $M(\sigma)$ has trace distance from ρ smaller than δ ,

$$QC_M^\delta(\rho) := \min \{ \ell(\sigma) \mid \|\rho - M(\sigma)\|_{\text{Tr}} \leq \delta \}. \quad (9)$$

⁴ We use the notations $\lfloor x \rfloor = \max\{n \in \mathbb{N} \mid n \leq x\}$ and $\lceil x \rceil = \min\{n \in \mathbb{N} \mid n \geq x\}$.

Similarly, we define an approximation-scheme quantum complexity $QC_M^{\searrow 0}$ by the minimal length $\ell(\sigma)$ of any density operator $\sigma \in \mathcal{T}_1^+(\mathcal{H}_{\{0,1\}}^*)$, such that when given M as input together with any integer k , the output $M(k, \sigma)$ has trace distance from ρ smaller than $1/k$:

$$QC_M^{\searrow 0}(\rho) := \min \left\{ \ell(\sigma) \mid \|\rho - M(k, \sigma)\|_{\text{Tr}} \leq \frac{1}{k} \text{ for every } k \in \mathbb{N} \right\}. \quad (10)$$

Some points are worth stressing in connection with the previous definition:

- This definition is essentially equivalent to the definition given by Berthiaume et. al. in [5]. The only technical difference is that we found it convenient to use the trace distance rather than the fidelity.
- The *same* qubit program σ is accompanied by a classical specification of an integer k , which tells the program to what accuracy the computation of the output state must be accomplished.
- If M does not have too restricted functionality (for example, if M is universal, which is discussed below), a noiseless transmission channel (implementing the identity transformation) between the input and output tracks can always be realized: this corresponds to classical literal transcription, so that automatically $QC_M^\delta(\rho) \leq \ell(\rho) + c_M$ for some constant c_M . Of course, the key point in classical as well as quantum algorithmic complexity is that there are sometimes much shorter qubit programs than literal transcription.
- The exact choice of the accuracy specification $\frac{1}{k}$ is not important; we can choose any computable function that tends to zero for $k \rightarrow \infty$, and we will always get an equivalent definition (in the sense of being equal up to some constant).

The same is true for the choice of the encoding \mathcal{C} : As long as k and σ can both be computably decoded from $\mathcal{C}(k, \sigma)$ and as long as there is no way to extract additional information on the desired output ρ from the k -description part of $\mathcal{C}(k, \sigma)$, the results will be equivalent up to some constant.

Both quantum algorithmic complexities QC^δ and $QC^{\searrow 0}$ are related to each other in a useful way:

Lemma 2 (Relation between Q-Complexities). *For every QTM M and every $k \in \mathbb{N}$, we have the relation*

$$QC_M^{1/k}(\rho) \leq QC_M^{\searrow 0}(\rho) + 2\lfloor \log k \rfloor + 2, \quad \rho \in \mathcal{T}_1^+(\mathcal{H}_{\{0,1\}}^*). \quad (11)$$

Proof. Suppose that $QC_M^{\searrow 0}(\rho) = l$, so there is a density matrix $\sigma \in \mathcal{T}_1^+(\mathcal{H}_{\{0,1\}}^*)$ with $\ell(\sigma) = l$, such that $\|M(k, \sigma) - \rho\|_{\text{Tr}} \leq \frac{1}{k}$ for every $k \in \mathbb{N}$. Then $\sigma' := \mathcal{C}(k, \sigma)$, where \mathcal{C} is given in Definition 2, is an input for M such that $\|M(\sigma') - \rho\|_{\text{Tr}} \leq \frac{1}{k}$. Thus $QC_M^{1/k}(\rho) \leq \ell(\sigma') \leq 2\lfloor \log k \rfloor + 2 + \ell(\sigma) = 2\lfloor \log k \rfloor + 2 + QC_M^{\searrow 0}(\rho)$, where the second inequality is by (8). \square

The term $2\lfloor \log k \rfloor + 2$ in (11) depends on our encoding \mathcal{C} given in Definition 2, but if M is assumed to be universal (which will be discussed below), then (11) will hold for *every* encoding, if we replace the term $2\lfloor \log k \rfloor + 2$ by $K(k) + c_M$, where $K(k) \leq 2\lfloor \log k \rfloor + \mathcal{O}(1)$ denotes the classical (self-delimiting) algorithmic complexity of the integer k , and c_M is some constant depending only on M . For more details we refer the reader to [26].

In [4], it is proved that there is a universal QTM ($UQTM$) \mathfrak{U} that can simulate with arbitrary accuracy every other machine M in the sense that for every such M there is a classical bit string $\bar{M} \in \{0, 1\}^*$ such that

$$\|\mathfrak{U}(\bar{M}, \sigma, k, t) - M_{\mathbf{O}}^t(\sigma)\|_{\text{Tr}} \leq \frac{1}{k} \quad \text{for every } \sigma \in \mathcal{T}_1^+(\mathcal{H}_{\{0,1\}^*}), \quad (12)$$

where $k, t \in \mathbb{N}$. As it is implicit in this definition of universality, we will demand that \mathfrak{U} is able to perfectly simulate every classical computation, and that it can apply a given unitary transformation within any desired accuracy (it is shown in [4] that such machines exist).

We choose an arbitrary $UQTM$ \mathfrak{U} which is constructed such that it decodes our encoding $\mathcal{C}(k, \sigma)$ given in Definition 2 into k and σ at the beginning of the computation. Like in the classical case, we fix \mathfrak{U} for the rest of the paper and simplify notation by

$$QC^{\searrow 0}(\rho) := QC_{\mathfrak{U}}^{\searrow 0}(\rho), \quad QC^{\delta}(\rho) := QC_{\mathfrak{U}}^{\delta}(\rho) .$$

5. Proof of the Main Theorem

As already mentioned at the beginning of Section 2, without loss of generality, we give the proofs for the case that \mathcal{A} is the algebra of the observables of a qubit, i.e. the complex 2×2 -matrices.

5.1. Lower Bound. For classical TMs , there are no more than $2^{c+1} - 1$ different programs of length $\ell \leq c$. This can be used as a "counting argument" for proving the lower bound of Brudno's Theorem in the classical case ([22]). We are now going to prove a similar statement for QTM s.

Our first step is to elaborate on an argument due to [5] which states that there cannot be more than $2^{\ell+1} - 1$ mutually orthogonal one-dimensional projectors p with quantum complexity $QC^{\searrow 0}(p) \leq \ell$. The argument is based on Holevo's χ -quantity associated to any ensemble $\mathbb{E}_{\rho} := \{\lambda_i, \rho_i\}_i$ consisting of weights $0 \leq \lambda_i \leq 1$, $\sum_i \lambda_i = 1$, and of density matrices ρ_i acting on a Hilbert space \mathcal{H} . Setting $\rho := \sum_i \lambda_i \rho_i$, the χ -quantity is defined as follows

$$\chi(\mathbb{E}_{\rho}) := S(\rho) - \sum_i \lambda_i S(\rho_i) \quad (13)$$

$$= \sum_i \lambda_i S(\rho_i, \rho) , \quad (14)$$

where, in the second line, the relative entropy appears

$$S(\rho_1, \rho_2) := \begin{cases} \text{Tr}(\rho_1 (\log \rho_1 - \log \rho_2)) & \text{if } \text{supp } \rho_1 \leq \text{supp } \rho_2 , \\ \infty & \text{otherwise.} \end{cases} \quad (15)$$

If $\dim(\mathcal{H})$ is finite, (13) is bounded by the maximal von Neumann entropy:

$$\chi(\mathbb{E}_{\rho}) \leq S(\rho) \leq \log \dim(\mathcal{H}). \quad (16)$$

In the following, \mathcal{H}' denotes an arbitrary (possibly infinite-dimensional) Hilbert space, while the rest of the notation is adopted from Subsection 4.2.

Lemma 3 (Quantum Counting Argument). *Let $0 < \delta < 1/e$, $c \in \mathbb{N}$ such that $c \geq \frac{2}{\delta} (2 + \log \frac{1}{\delta})$, P an orthogonal projector onto a linear subspace of an arbitrary Hilbert space \mathcal{H}' , and $\mathcal{E} : \mathcal{T}_1^+(\mathcal{H}_{\{0,1\}^*}) \rightarrow \mathcal{T}_1^+(\mathcal{H}')$ a quantum operation. Let N_c^δ be a subset of one-dimensional mutually orthogonal projections from the set*

$$A_c^\delta(\mathcal{E}, P) := \{p \leq P \mid p \text{ 1-dim. proj.}, \exists \sigma \in \mathcal{T}_1^+(\mathcal{H}_{\leq c}) : \|\mathcal{E}(\sigma) - p\|_{\text{Tr}} \leq \delta\},$$

that is, the set of all pure quantum states which are reproduced within δ by the operation \mathcal{E} on some input of length $\leq c$. Then it holds that

$$\log |N_c^\delta| < c + 1 + \frac{2 + \delta}{1 - 2\delta} \delta c .$$

Proof. Let $p_j \in A_c^\delta(\mathcal{E}, P)$, $j = 1, \dots, N$, be a set of mutually orthogonal projectors and $p_{N+1} := \mathbf{1}_{\mathcal{H}'} - \sum_{i=1}^N p_i$. By the definition of $A_c^\delta(\mathcal{E}, P)$, for every $1 \leq i \leq N$, there are density matrices $\sigma_i \in \mathcal{T}_1^+(\mathcal{H}_{\leq c})$ with

$$\|\mathcal{E}(\sigma_i) - p_i\|_{\text{Tr}} \leq \delta . \quad (17)$$

Consider the equidistributed ensemble $\mathbb{E}_\sigma := \left\{ \frac{1}{N}, \sigma_i \right\}$, where $\sigma := \frac{1}{N} \sum_{i=1}^N \sigma_i$ also acts on $\mathcal{H}_{\leq c}$. Using that $\dim \mathcal{H}_{\leq c} = 2^{c+1} - 1$, inequality (16) yields

$$\chi(\mathbb{E}_\sigma) < c + 1. \quad (18)$$

We define a quantum operation \mathcal{R} on $\mathcal{T}_1^+(\mathcal{H}')$ by $\mathcal{R}(a) := \sum_{i=1}^{N+1} p_i a p_i$. Applying twice the monotonicity of the relative entropy under quantum operations, we obtain

$$\frac{1}{N} \sum_{i=1}^N S(\mathcal{R} \circ \mathcal{E}(\sigma_i), \mathcal{R} \circ \mathcal{E}(\sigma)) \leq \frac{1}{N} \sum_{i=1}^N S(\mathcal{E}(\sigma_i), \mathcal{E}(\sigma)) \leq \chi(\mathbb{E}_\sigma) . \quad (19)$$

Moreover, for every $i \in \{1, \dots, N\}$, the density operator $\mathcal{R} \circ \mathcal{E}(\sigma_i)$ is close to the corresponding one-dimensional projector $\mathcal{R}(p_i) = p_i$. Indeed, by the contractivity of the trace distance under quantum operations (compare Thm. 9.2 in [29]) and by assumption (17), it holds

$$\|\mathcal{R} \circ \mathcal{E}(\sigma_i) - p_i\|_{\text{Tr}} \leq \|\mathcal{E}(\sigma_i) - p_i\|_{\text{Tr}} \leq \delta .$$

Let $\Delta := \frac{1}{N} \sum_{i=1}^N p_i$. The trace-distance is convex ([29], (9.51)), thus

$$\|\mathcal{R} \circ \mathcal{E}(\sigma) - \Delta\|_{\text{Tr}} \leq \frac{1}{N} \sum_{i=1}^N \|\mathcal{R} \circ \mathcal{E}(\sigma_i) - p_i\|_{\text{Tr}} \leq \delta ,$$

whence, since $\delta < \frac{1}{e}$, Fannes' inequality (compare Thm. 11.6 in [29]) gives

$$\begin{aligned} S(\mathcal{R} \circ \mathcal{E}(\sigma_i)) &= |S(\mathcal{R} \circ \mathcal{E}(\sigma_i)) - S(p_i)| \leq \delta \log(N+1) + \eta(\delta) \\ \text{and } |S(\mathcal{R} \circ \mathcal{E}(\sigma)) - S(\Delta)| &\leq \delta \log(N+1) + \eta(\delta) , \end{aligned}$$

where $\eta(\delta) := -\delta \log \delta$. Combining the two estimates above with (18) and (19), we obtain

$$\begin{aligned}
c + 1 &> \chi(\mathbb{E}_\sigma) \geq S(\mathcal{R} \circ \mathcal{E}(\sigma)) - \frac{1}{N} \sum_{i=1}^N S(\mathcal{R} \circ \mathcal{E}(\sigma_i)) \\
&\geq S(\Delta) - \delta \log(N+1) - \eta(\delta) - \frac{1}{N} \sum_{i=1}^N (\delta \log(N+1) + \eta(\delta)) \\
&= \log N - 2\delta \log(N+1) - 2\eta(\delta) \\
&\geq (1-2\delta) \log N - 2\delta - 2\eta(\delta).
\end{aligned} \tag{20}$$

Assume now that $\log N \geq c + 1 + \frac{2+\delta}{1-2\delta} \delta c$. Then it follows (20) that $c < \frac{2}{\delta} (2 + \log \frac{1}{\delta})$. So if c is larger than this expression, the maximum number $|N_c^\delta|$ of mutually orthogonal projectors in $A_c^\delta(\mathcal{E}, P)$ must be bounded by $\log |N_c^\delta| < c + 1 + \frac{2+\delta}{1-2\delta} \delta c$. \square

The second step uses the previous lemma together with the following theorem [7, Prop. 2.1]. It is closely related to the quantum Shannon-McMillan Theorem and concerns the minimal dimension of the Ψ -typical subspaces.

Theorem 2. *Let $(\mathcal{A}^\infty, \Psi)$ be an ergodic quantum source with entropy rate s . Then, for every $0 < \varepsilon < 1$,*

$$\lim_{n \rightarrow \infty} \frac{1}{n} \beta_{\varepsilon, n}(\Psi) = s, \tag{21}$$

where $\beta_{\varepsilon, n}(\Psi) := \min \{ \log \text{Tr}_n(q) \mid q \in \mathcal{A}^{(n)} \text{ projector, } \Psi^{(n)}(q) \geq 1 - \varepsilon \}$.

Notice that the limit (21) is valid for all $0 < \varepsilon < 1$. By means of this property, we will first prove the lower bound for the finite-accuracy complexity QC^δ , and then use Lemma 2 to extend it to $QC^{\searrow 0}$.

Corollary 1 (Lower Bound for $\frac{1}{n} QC^\delta$).

Let $(\mathcal{A}^\infty, \Psi)$ be an ergodic quantum source with entropy rate s . Moreover, let $0 < \delta < 1/e$, and let $(p_n)_{n \in \mathbb{N}}$ be a sequence of Ψ -typical projectors. Then, there is another sequence of Ψ -typical projectors $q_n(\delta) \leq p_n$, such that for n large enough

$$\frac{1}{n} QC^\delta(q) > s - \delta(2 + \delta)s$$

is true for every one-dimensional projector $q \leq q_n(\delta)$.

Proof. The case $s = 0$ is trivial, so let $s > 0$. Fix $n \in \mathbb{N}$ and some $0 < \delta < 1/e$, and consider the set

$$\tilde{A}_n(\delta) := \{ p \leq p_n \mid p \text{ one-dim. proj., } QC^\delta(p) \leq ns(1 - \delta(2 + \delta)) \}.$$

From the definition of $QC^\delta(p)$, to all p 's there exist associated density matrices σ_p with $\ell(\sigma_p) \leq ns(1 - \delta(2 + \delta))$ such that $\|\mathcal{M}(\sigma_p) - p\|_{\text{Tr}} \leq \delta$, where \mathcal{M}

denotes the quantum operation $\mathcal{M} : \mathcal{T}_1^+(\mathcal{H}_{\{0,1\}^*}) \rightarrow \mathcal{T}_1^+(\mathcal{H}_{\{0,1\}^*})$ of the corresponding $UQTM \mathfrak{U}$, as explained in Lemma 1. Using the notation of Lemma 3, it thus follows that

$$\tilde{A}_n(\delta) \subset A_{\lceil ns(1-\delta(2+\delta)) \rceil}^\delta(\mathcal{M}, p_n).$$

Let $p_n(\delta) \leq p_n$ be a sum of a maximal number of mutually orthogonal projectors from $A_{\lceil ns(1-\delta(2+\delta)) \rceil}^\delta(\mathcal{M}, p_n)$. If n was chosen large enough such that $ns(1-\delta(2+\delta)) \geq \frac{1}{\delta}(4 + 2 \log \frac{1}{\delta})$ is satisfied, Lemma 3 implies that

$$\log \text{Tr } p_n(\delta) < \lceil ns(1-\delta(2+\delta)) \rceil + 1 + \frac{2+\delta}{1-2\delta} \delta \lceil ns(1-\delta(2+\delta)) \rceil, \quad (22)$$

and there are no one-dimensional projectors $p \leq p_n(\delta)^\perp := p_n - p_n(\delta)$ such that $p \in A_{\lceil ns(1-\delta(2+\delta)) \rceil}^\delta(\mathcal{M}, p_n)$. Namely, one-dimensional projectors $p \leq p_n(\delta)^\perp$ must satisfy $\frac{1}{n}QC^\delta(p) > s - \delta(2+\delta)s$. Since inequality (22) is valid for every $n \in \mathbb{N}$ large enough, we conclude

$$\limsup_{n \rightarrow \infty} \frac{1}{n} \log \text{Tr } p_n(\delta) \leq s - 2\delta^3 s - \frac{5\delta^4 s}{1-2\delta} < s. \quad (23)$$

Using Theorem 2, we obtain that $\lim_{n \rightarrow \infty} \Psi^{(n)}(p_n(\delta)) = 0$. Finally, set $q_n(\delta) := p_n(\delta)^\perp$. The claim follows. \square

Corollary 2 (Lower Bound for $\frac{1}{n}QC^{\searrow 0}$).

Let $(\mathcal{A}^\infty, \Psi)$ be an ergodic quantum source with entropy rate s . Let $(p_n)_{n \in \mathbb{N}}$ with $p_n \in \mathcal{A}^{(n)}$ be an arbitrary sequence of Ψ -typical projectors. Then, for every $0 < \delta < 1/e$, there is a sequence of Ψ -typical projectors $q_n(\delta) \leq p_n$ such that for n large enough

$$\frac{1}{n}QC^{\searrow 0}(q) > s - \delta$$

is satisfied for every one-dimensional projector $q \leq q_n(\delta)$.

Proof. According to Corollary 1, for every $k \in \mathbb{N}$, there exists a sequence of Ψ -typical projectors $p_n(\frac{1}{k}) \leq p_n$ with $\frac{1}{n}QC^{\frac{1}{k}}(q) > s - \frac{1}{k}(2 + \frac{1}{k})s$ for every one-dimensional projector $q \leq p_n(\frac{1}{k})$ if n is large enough. We have

$$\begin{aligned} \frac{1}{n}QC^{\searrow 0}(q) &\geq \frac{1}{n}QC^{1/k}(q) - \frac{2 + 2\lfloor \log k \rfloor}{n} \\ &> s - \frac{1}{k} \left(2 + \frac{1}{k} \right) s - \frac{2(2 + \log k)}{n}, \end{aligned}$$

where the first estimate is by Lemma 2, and the second one is true for one-dimensional projectors $q \leq p_n(\frac{1}{k})$ and $n \in \mathbb{N}$ large enough. Fix a large k satisfying $\frac{1}{k}(2 + \frac{1}{k})s \leq \frac{\delta}{2}$. The result follows by setting $q_n(\delta) = p_n(\frac{1}{k})$. \square

5.2. Upper Bound. In the previous section, we have shown that with high probability and for large m , the finite-accuracy complexity rate $\frac{1}{m}QC^\delta$ is bounded from below by $s(1 - \delta(2 + \delta))$, and the approximation-scheme quantum complexity rate $\frac{1}{m}QC^{\searrow 0}$ by $s - \delta$. We are now going to establish the upper bounds.

Proposition 1 (Upper Bound).

Let $(\mathcal{A}^\infty, \Psi)$ be an ergodic quantum source with entropy rate s . Then, for every $0 < \delta < 1/e$, there is a sequence of Ψ -typical projectors $q_m(\delta) \in \mathcal{A}^{(m)}$ such that for every one-dimensional projector $q \leq q_m(\delta)$ and m large enough

$$\frac{1}{m}QC^{\searrow 0}(q) < s + \delta \quad \text{and} \quad (24)$$

$$\frac{1}{m}QC^\delta(q) < s + \delta. \quad (25)$$

We prove the above proposition by explicitly providing a quantum algorithm (with program length increasing like $m(s + \delta)$) that computes q within arbitrary accuracy. This will be done by means of quantum universal typical subspaces constructed by Kaltchenko and Yang in [21].

Theorem 3 (Universal Typical Subspaces).

Let $s > 0$ and $\varepsilon > 0$. There exists a sequence of projectors $Q_{s,\varepsilon}^{(n)} \in \mathcal{A}^{(n)}$, $n \in \mathbb{N}$, such that for n large enough

$$\text{Tr}(Q_{s,\varepsilon}^{(n)}) \leq 2^{n(s+\varepsilon)} \quad (26)$$

and for every ergodic quantum state $\Psi \in \mathcal{S}(\mathcal{A}^\infty)$ with entropy rate $s(\Psi) \leq s$ it holds that

$$\lim_{n \rightarrow \infty} \Psi^{(n)}(Q_{s,\varepsilon}^{(n)}) = 1. \quad (27)$$

We call the orthogonal projectors $Q_{s,\varepsilon}^{(n)}$ in the above theorem universal typical projectors at level s . Suited for designing an appropriate quantum algorithm, we slightly modify the proof given by Kaltchenko and Yang in [21].

Proof. Let $l \in \mathbb{N}$ and $R > 0$. We consider an Abelian quasi-local subalgebra $\mathcal{C}_l^\infty \subseteq \mathcal{A}^\infty$ constructed from a maximal Abelian l -block subalgebra $\mathcal{C}_l \subseteq \mathcal{A}^{(l)}$. The results in [42, 23] imply that there exists a universal sequence of projectors $p_{l,R}^{(n)} \in \mathcal{C}_l^{(n)} \subseteq \mathcal{A}^{(ln)}$ with $\frac{1}{n} \log \text{Tr } p_{l,R}^{(n)} \leq R$ such that $\lim_{n \rightarrow \infty} \pi^{(n)}(p_{l,R}^{(n)}) = 1$ for any ergodic state π on the Abelian algebra \mathcal{C}_l^∞ with entropy rate $s(\pi) < R$. Notice that ergodicity and entropy rate of π are defined with respect to the shift on \mathcal{C}_l^∞ , which corresponds to the l -shift on \mathcal{A}^∞ .

The first step in [21] is to apply unitary operators of the form $U^{\otimes n}$, $U \in \mathcal{A}^{(l)}$ unitary, to the $p_{l,R}^{(n)}$ and to introduce the projectors

$$w_{l,R}^{(ln)} := \bigvee_{U \in \mathcal{A}^{(l)} \text{ unitary}} U^{\otimes n} p_{l,R}^{(n)} U^{*\otimes n} \in \mathcal{A}^{(ln)}. \quad (28)$$

Let $p_{l,R}^{(n)} = \sum_{i \in I} |i_{l,R}^{(n)}\rangle \langle i_{l,R}^{(n)}|$ be a spectral decomposition of $p_{l,R}^{(n)}$ (with $I \subset \mathbb{N}$ some index set), and let $\mathbf{P}(V)$ denote the orthogonal projector onto a given subspace V . Then, $w_{l,R}^{(ln)}$ can also be written as

$$w_{l,R}^{(ln)} = \mathbf{P} \left(\text{span}\{U^{\otimes n} |i_{l,R}^{(n)}\rangle : i \in I, U \in \mathcal{A}^{(l)} \text{ unitary}\} \right).$$

It will be more convenient for the construction of our algorithm in 5.2.1 to consider the projector

$$W_{l,R}^{(ln)} := \mathbf{P} \left(\text{span}\{A^{\otimes n} |i_{l,R}^{(n)}\rangle : i \in I, A \in \mathcal{A}^{(l)}\} \right). \quad (29)$$

It holds that $w_{l,R}^{(ln)} \leq W_{l,R}^{(ln)}$. For integers $m = nl + k$ with $n \in \mathbb{N}$ and $k \in \{0, \dots, l-1\}$ we introduce the projectors in $\mathcal{A}^{(m)}$

$$w_{l,R}^{(m)} := w_{l,R}^{(ln)} \otimes \mathbf{1}^{\otimes k}, \quad W_{l,R}^{(m)} := W_{l,R}^{(ln)} \otimes \mathbf{1}^{\otimes k}. \quad (30)$$

We now use an argument of [20] to estimate the trace of $W_{l,R}^{(m)} \in \mathcal{A}^{(m)}$. The dimension of the symmetric subspace $\text{SYM}^n(\mathcal{A}^{(l)}) := \text{span}\{A^{\otimes n} : A \in \mathcal{A}^{(l)}\}$ is upper bounded by $(n+1)^{\dim \mathcal{A}^{(l)}}$, thus

$$\begin{aligned} \text{Tr } W_{l,R}^{(m)} &= \text{Tr } W_{l,R}^{(ln)} \cdot \text{Tr } \mathbf{1}^{\otimes k} \leq (n+1)^{2^{2l}} \text{Tr } p_{l,R}^{(n)} \cdot 2^l \\ &\leq (n+1)^{2^{2l}} \cdot 2^{Rn} \cdot 2^l. \end{aligned} \quad (31)$$

Now we consider a stationary ergodic state Ψ on the quasi-local algebra \mathcal{A}^∞ with entropy rate $s(\Psi) \leq s$. Let $\varepsilon, \delta > 0$. If l is chosen large enough then the projectors $w_{l,R}^{(m)}$, where $R := l(s + \frac{\varepsilon}{2})$, are δ -typical for Ψ , i.e. $\Psi^{(m)}(w_{l,R}^{(m)}) \geq 1 - \delta$, for $m \in \mathbb{N}$ sufficiently large. This can be seen as follows. Due to the result in [7, Thm. 3.1] the ergodic state Ψ convexly decomposes into $k(l) \leq l$ states

$$\Psi = \frac{1}{k(l)} \sum_{i=1}^{k(l)} \Psi_{i,l}, \quad (32)$$

each $\Psi_{i,l}$ being ergodic with respect to the l -shift on \mathcal{A}^∞ and having an entropy rate (with respect to the l -shift) equal to $s(\Psi) \cdot l$. We define for $\Delta > 0$ the set of integers

$$A_{l,\Delta} := \{i \in \{1, \dots, k(l)\} : S(\Psi_{i,l}^{(l)}) \geq l(s(\Psi) + \Delta)\}. \quad (33)$$

Then, according to a density lemma proven in [7, Lemma 3.1] it holds

$$\lim_{l \rightarrow \infty} \frac{|A_{l,\Delta}|}{k(l)} = 0. \quad (34)$$

Let $\mathcal{C}_{i,l}$ be the maximal Abelian subalgebra of $\mathcal{A}^{(l)}$ generated by the one-dimensional eigenprojectors of $\Psi_{i,l}^{(l)} \in \mathcal{S}(\mathcal{A}^{(l)})$. The restriction of a component

$\Psi_{i,l}$ to the Abelian quasi-local algebra $\mathcal{C}_{i,l}^\infty$ is again an ergodic state. It holds in general

$$l \cdot s(\Psi) = s(\Psi_{i,l}) \leq s(\Psi_{i,l} \upharpoonright \mathcal{C}_{i,l}^\infty) \leq S(\Psi_{i,l}^{(l)} \upharpoonright \mathcal{C}_{i,l}) = S(\Psi_{i,l}^{(l)}). \quad (35)$$

For $i \in A_{l,\Delta}^c$, where we set $\Delta := \frac{R}{l} - s(\Psi)$, we additionally have the upper bound $S(\Psi_{i,l}^{(l)}) < R$. Let $U_i \in \mathcal{A}^{(l)}$ be a unitary operator such that $U_i^{\otimes n} p_{l,R}^{(n)} U_i^{*\otimes n} \in \mathcal{C}_{i,l}^{(n)}$. For every $i \in A_{l,\Delta}^c$, it holds that

$$\Psi_{i,l}^{(ln)}(w_{l,R}^{(ln)}) \geq \Psi_{i,l}^{(ln)}(U_i^{\otimes n} p_{l,R}^{(n)} U_i^{*\otimes n}) \longrightarrow 1 \quad \text{as } n \rightarrow \infty. \quad (36)$$

We fix an $l \in \mathbb{N}$ large enough to fulfill $\frac{|A_{l,\Delta}^c|}{k(l)} \geq 1 - \frac{\delta}{2}$ and use the ergodic decomposition (32) to obtain the lower bound

$$\Psi^{(ln)}(w_{l,R}^{(ln)}) \geq \frac{1}{k(l)} \sum_{i \in A_{l,\Delta}^c} \Psi_{l,i}^{(nl)}(w_{l,R}^{(ln)}) \geq \left(1 - \frac{\delta}{2}\right) \min_{i \in A_{l,\Delta}^c} \Psi_{i,l}^{(nl)}(w_{l,R}^{(ln)}). \quad (37)$$

From (36) we conclude that for n large enough

$$\Psi^{(ln)}(W_{l,R}^{(ln)}) \geq \Psi^{(ln)}(w_{l,R}^{(ln)}) \geq 1 - \delta. \quad (38)$$

We proceed by following the lines of [21] by introducing the sequence l_m , $m \in \mathbb{N}$, where each l_m is a power of 2 fulfilling the inequality

$$l_m 2^{3 \cdot l_m} \leq m < 2l_m 2^{3 \cdot 2l_m}. \quad (39)$$

Let the integer sequence n_m and the real-valued sequence R_m be defined by $n_m := \lfloor \frac{m}{l_m} \rfloor$ and $R_m := l_m \cdot (s + \frac{\varepsilon}{2})$. Then we set

$$Q_{s,\varepsilon}^{(m)} := \begin{cases} W_{l_m, R_m}^{(l_m n_m)} & \text{if } m = l_m 2^{3 \cdot l_m}, \\ W_{l_m, R_m}^{(l_m n_m)} \otimes \mathbf{1}^{\otimes (m - l_m n_m)} & \text{otherwise.} \end{cases} \quad (40)$$

Observe that

$$\begin{aligned} \frac{1}{m} \log \text{Tr } Q_{s,\varepsilon}^{(m)} &\leq \frac{1}{n_m l_m} \log \text{Tr } Q_{s,\varepsilon}^{(m)} \\ &\leq \frac{4^{l_m} \log(n_m + 1)}{l_m n_m} + \frac{R_m}{l_m} + \frac{1}{n_m} \end{aligned} \quad (41)$$

$$\leq \frac{4^{l_m} (6l_m + 2)}{l_m 2^{3l_m} - 1} + s + \frac{\varepsilon}{2} + \frac{1}{2^{3l_m} - 1}, \quad (42)$$

where the second inequality is by estimate (31) and the last one by the bounds on n_m

$$2^{3l_m} - 1 \leq \frac{m}{l_m} - 1 \leq n_m \leq \frac{m}{l_m} \leq 2^{6l_m + 1}.$$

Thus, for large m , it holds

$$\frac{1}{m} \log \text{Tr } Q_{s,\varepsilon}^{(m)} \leq s + \varepsilon. \quad (43)$$

By the special choice (39) of l_m it is ensured that the sequence of projectors $Q_{s,\varepsilon}^{(m)} \in \mathcal{A}^{(m)}$ is indeed typical for any quantum state Ψ with entropy rate $s(\Psi) \leq s$, compare [21]. This means that $\{Q_{s,\varepsilon}^{(m)}\}_{m \in \mathbb{N}}$ is a sequence of universal typical projectors at level s . \square

5.2.1. Construction of the Decompression Algorithm. We proceed by applying the latter result to universal typical subspaces for our proof of the upper bound. Let $0 < \varepsilon < \delta/2$ be an arbitrary real number such that $r := s + \varepsilon$ is rational, and let $q_m := Q_{s,\varepsilon}^{(m)}$ be the universal projector sequence of Theorem 3. Recall that the projector sequence q_m is *independent* of the choice of the ergodic state Ψ , as long as $s(\Psi) \leq s$.

Because of (26), for m large enough, there exists some unitary transformation U^* that transforms the projector q_m into a projector belonging to $\mathcal{T}_1^+(\mathcal{H}_{\lceil mr \rceil})$, thus transforming every one-dimensional projector $q \leq q_m$ into a qubit string $\tilde{q} := U^* q U$ of length $\ell(\tilde{q}) = \lceil mr \rceil$.

As shown in [4], a *UQTM* can implement every classical algorithm, and it can apply every unitary transformation U (when given an algorithm for the computation of U) on its tapes within any desired accuracy. We can thus feed \tilde{q} (plus some classical instructions including a subprogram for the computation of U) as input into the *UQTM* \mathfrak{A} . This *UQTM* starts by computing a classical description of the transformation U , and subsequently applies U to \tilde{q} , recovering the original projector $q = U \tilde{q} U^*$ on the output tape.

Since $U = U(q_m)$ depends on Ψ only through its entropy rate $s(\Psi)$, the subprogram that computes U does not have to be supplied with additional information on Ψ and will thus have fixed length.

We give a precise definition of a quantum decompression algorithm \mathfrak{A} , which is, formally, a mapping (r is rational)

$$\begin{aligned} \mathfrak{A} : \mathbb{N} \times \mathbb{N} \times \mathbb{Q} \times \mathcal{H}_{\{0,1\}^*} &\rightarrow \mathcal{H}_{\{0,1\}^*} , \\ (k, m, r, \tilde{q}) &\mapsto q = \mathfrak{A}(k, m, r, \tilde{q}) . \end{aligned}$$

We require that \mathfrak{A} is a "short algorithm" in the sense of "short in description", *not* short (fast) in running time or resource consumption. Indeed, the algorithm \mathfrak{A} is very slow and memory consuming, but this does not matter, since Kolmogorov complexity only cares about the description length of the program.

The instructions defining the quantum algorithm \mathfrak{A} are:

1. Read the value of m , and find a solution $l \in \mathbb{N}$ for the inequality

$$l \cdot 2^{3l} \leq m < 2 \cdot l \cdot 2^{3 \cdot 2l}$$

such that l is a power of two. (There is only one such l .)

2. Compute $n := \lfloor \frac{m}{l} \rfloor$.
3. Read the value of r . Compute $R := l \cdot r$.
4. Compute a list of codewords $\Omega_{l,R}^{(n)}$, belonging to a classical universal block code sequence of rate R . (For the construction of an appropriate algorithm, see [23, Thm. 2 and 1].) Since

$$\Omega_{l,R}^{(n)} \subset (\{0,1\}^l)^n ,$$

$\Omega_{l,R}^{(n)} = \{\omega_1, \omega_2, \dots, \omega_M\}$ can be stored as a list of binary strings. Every string has length $\ell(\omega_i) = nl$. (Note that the exact value of the cardinality $M \approx 2^{nR}$ depends on the choice of $\Omega_{l,R}^{(n)}$.)

During the following steps, the quantum algorithm \mathfrak{A} will have to deal with

- rational numbers,
- square roots of rational numbers,
- binary-digit-approximations (up to some specified accuracy) of real numbers,
- (large) vectors and matrices containing such numbers.

A classical *TM* can of course deal with all such objects (and so can *QTM*): For example, rational numbers can be stored as a list of two integers (containing numerator and denominator), square roots can be stored as such a list and an additional bit denoting the square root, and binary-digit-approximations can be stored as binary strings. Vectors and matrices are arrays containing those objects. They are always assumed to be given in the computational basis. Operations on those objects, like addition or multiplication, are easily implemented.

The quantum algorithm \mathfrak{A} continues as follows:

5. Compute a basis $\{A_{\{i_1, \dots, i_n\}}\}$ of the symmetric subspace

$$\text{SYM}^n(\mathcal{A}^{(l)}) := \text{span}\{A^{\otimes n} : A \in \mathcal{A}^{(l)}\}.$$

This can be done as follows: For every n -tuple $\{i_1, \dots, i_n\}$, where $i_k \in \{1, \dots, 2^{2l}\}$, there is one basis element $A_{\{i_1, \dots, i_n\}} \in \mathcal{A}^{(ln)}$, given by the formula

$$A_{\{i_1, \dots, i_n\}} = \sum_{\sigma} e_{\sigma(i_1, \dots, i_n)}^{(l,n)}, \quad (44)$$

where the summation runs over all n -permutations σ , and

$$e_{i_1, \dots, i_n}^{(l,n)} := e_{i_1}^{(l)} \otimes e_{i_2}^{(l)} \otimes \dots \otimes e_{i_n}^{(l)},$$

with $\{e_k^{(l)}\}_{k=1}^{2^{2l}}$ a system of matrix units⁵ in $\mathcal{A}^{(l)}$.

There is a number of $d = \binom{n+2^{2l}-1}{2^{2l}-1} = \dim(\text{SYM}^n(\mathcal{A}^{(l)}))$ different matrices $A_{\{i_1, \dots, i_n\}}$ which we can label by $\{A_k\}_{k=1}^d$. It follows from (44) that these matrices have integer entries.

They are stored as a list of $2^{ln} \times 2^{ln}$ -tables of integers. Thus, this step of the computation is exact, that is without approximations.

6. For every $i \in \{1, \dots, M\}$ and $k \in \{1, \dots, d\}$, let

$$|u_{k,i}\rangle := A_k |\omega_i\rangle,$$

where $|\omega_i\rangle$ denotes the computational basis vector which is a tensor product of $|0\rangle$'s and $|1\rangle$'s according to the bits of the string ω_i . Compute the vectors $|u_{k,i}\rangle$ one after the other. For every vector that has been computed, check if it can be written as a linear combination of already computed vectors. (The corresponding system of linear equations can be solved exactly, since every

⁵ In the computational basis, all entries are zero, except for one entry which is one.

vector is given as an array of integers.) If yes, then discard the new vector $|u_{k,i}\rangle$, otherwise store it and give it a number.

This way, a set of vectors $\{|u_k\rangle\}_{k=1}^D$ is computed. These vectors linearly span the support of the projector $W_{l,R}^{(ln)}$ given in (29).

7. Denote by $\{|\phi_i\rangle\}_{i=1}^{2^{m-ln}}$ the computational basis vectors of \mathcal{H}_{m-ln} . If $m = l \cdot 2^{3 \cdot l}$, then let $\tilde{D} := D$, and let $|x_k\rangle := |u_k\rangle$. Otherwise, compute $|u_k\rangle \otimes |\phi_i\rangle$ for every $k \in \{1, \dots, D\}$ and $i \in \{1, \dots, 2^{m-ln}\}$. The resulting set of vectors $\{|x_k\rangle\}_{k=1}^{\tilde{D}}$ has cardinality $\tilde{D} := D \cdot 2^{m-ln}$.

In both cases, the resulting vectors $|x_k\rangle \in \mathcal{H}_m$ will span the support of the projector $Q_{s,\varepsilon}^{(m)} = q_m$.

8. The set $\{|x_k\rangle\}_{k=1}^{\tilde{D}}$ is completed to linearly span the whole space \mathcal{H}_m . This will be accomplished as follows:
Consider the sequence of vectors

$$(|\tilde{x}_1\rangle, |\tilde{x}_2\rangle, \dots, |\tilde{x}_{\tilde{D}+2^m}\rangle) := (|x_1\rangle, |x_2\rangle, \dots, |x_{\tilde{D}}\rangle, |\Phi_1\rangle, |\Phi_2\rangle, \dots, |\Phi_{2^m}\rangle),$$

where $\{|\Phi_k\rangle\}_{k=1}^{2^m}$ denotes the computational basis vectors of \mathcal{H}_m . Find the smallest i such that $|\tilde{x}_i\rangle$ can be written as a linear combination of $|\tilde{x}_1\rangle, |\tilde{x}_2\rangle, \dots, |\tilde{x}_{i-1}\rangle$, and discard it (this can still be decided exactly, since all the vectors are given as tables of integers). Repeat this step \tilde{D} times until there remain only 2^m linearly independent vectors, namely all the $|x_j\rangle$ and $2^m - \tilde{D}$ of the $|\Phi_j\rangle$.

9. Apply the Gram-Schmidt orthonormalization procedure to the resulting vectors, to get an orthonormal basis $\{|y_k\rangle\}_{k=1}^{2^m}$ of \mathcal{H}_m , such that the first \tilde{D} vectors are a basis for the support of $Q_{s,\varepsilon}^{(m)} = q_m$.
Since every vector $|x_j\rangle$ and $|\Phi_j\rangle$ has only integer entries, all the resulting vectors $|y_k\rangle$ will have only entries that are (plus or minus) the square root of some rational number.

Up to this point, every calculation was *exact* without any numerical error, comparable to the way that well-known computer algebra systems work. The goal of the next steps is to compute an approximate description of the desired unitary decompression map U and subsequently apply it to the quantum state \tilde{q} .

According to Section 6 in [4], a *UQTM* is able to apply a unitary transformation U on some segment of its tape within an accuracy of δ , if it is supplied with a complex matrix \tilde{U} as input which is within operator norm distance $\frac{\delta}{2(10\sqrt{d})^d}$ of U (here, d denotes the size of the matrix). Thus, the next task is to compute the number of digits N that are necessary to guarantee that the output will be within trace distance $\delta = \frac{1}{k}$ of q .

10. Read the value of k (which denotes an approximation parameter; the larger k , the more accurate the output of the algorithm will be). Due to the considerations above and the calculations below, the necessary number of digits N turns out to be $N = 1 + \lceil \log(2k2^m(10\sqrt{2^m})^{2^m}) \rceil$. Compute this number.

Afterwards, compute the components of all the vectors $\{|y_k\rangle\}_{k=1}^{2^m}$ up to N binary digits of accuracy. (This involves only calculation of the square root of rational numbers, which can easily be done to any desired accuracy.)

Call the resulting numerically approximated vectors $|\tilde{y}_k\rangle$. Write them as columns into an array (a matrix) $\tilde{U} := (\tilde{y}_1, \tilde{y}_2, \dots, \tilde{y}_{2^m})$.

Let $U := (y_1, y_2, \dots, y_{2^m})$ denote the unitary matrix with the exact vectors $|y_k\rangle$ as columns. Since N binary digits give an accuracy of 2^{-N} , it follows that

$$|\tilde{U}_{i,j} - U_{i,j}| < 2^{-N} < \frac{1/k}{2 \cdot 2^m (10\sqrt{2^m})^{2^m}}.$$

If two $2^m \times 2^m$ -matrices U and \tilde{U} are ε -close in their entries, they also must be $2^m \cdot \varepsilon$ -close in norm, so we get

$$\|\tilde{U} - U\| < \frac{1/k}{2(10\sqrt{2^m})^{2^m}}.$$

So far, every step was purely classical and could have been done on a classical computer. Now, the quantum part begins: \tilde{q} will be touched for the first time.

11. Compute $\lceil mr \rceil$, which gives the length $\ell(\tilde{q})$. Afterwards, move \tilde{q} to some free space on the input tape, and append zeroes, i.e. create the state

$$q' \equiv |\psi_0\rangle\langle\psi_0| := (|0\rangle\langle 0|)^{\otimes(m-\ell(\tilde{q}))} \otimes \tilde{q}$$

on some segment of m cells on the input tape.

12. Approximately apply the unitary transformation U on the tape segment that contains the state q' .

The machine cannot apply U exactly (since it only knows an approximation \tilde{U}), and it also cannot apply \tilde{U} directly (since \tilde{U} is only approximately unitary, and the machine can only do unitary transformations). Instead, it will effectively apply another unitary transformation V which is close to \tilde{U} and thus close to U , such that

$$\|V - U\| < \frac{1}{k}.$$

Let $|\psi\rangle := U|\psi_0\rangle$ be the output that we want to have, and let $|\phi\rangle := V|\psi_0\rangle$ be the approximation that is really computed by the machine. Then,

$$\| |\phi\rangle - |\psi\rangle \| < \frac{1}{k}.$$

A simple calculation proves that the trace distance must then also be small:

$$\| |\phi\rangle\langle\phi| - |\psi\rangle\langle\psi| \|_{\text{Tr}} < \frac{1}{k}.$$

14. Move $q := |\phi\rangle\langle\phi|$ to the output tape and halt.

5.2.2. Proof of Proposition 1. We have to give a precise definition how the parameters (m, r, \tilde{q}) are encoded into a single qubit string σ . (According to the definition of $QC^{\searrow 0}$, the parameter k is not a part of σ , but is given as a second parameter. See Definitions 2 and 3 for details.)

We choose to encode m by giving $\lfloor \log m \rfloor$ 1's, followed by one 0, followed by the $\lfloor \log m \rfloor + 1$ binary digits of m . Let $|M\rangle\langle M|$ denote the corresponding projector in the computational basis.

The parameter r can be encoded in any way, since it does not depend on m . The only constraint is that the description must be self-delimiting, i.e. it must be clear and decidable at what position the description for r starts and ends. The descriptions will also be given by a computational basis vector (or rather the corresponding projector) $|R\rangle\langle R|$.

The descriptions are then stuck together, and the input $\sigma(\tilde{q})$ is given by

$$\sigma(\tilde{q}) := |M\rangle\langle M| \otimes |R\rangle\langle R| \otimes \tilde{q}.$$

If m is large enough such that (43) is fulfilled, it follows that $\ell(\sigma(\tilde{q})) = 2\lfloor \log m \rfloor + 2 + c + \lceil mr \rceil$, where $c \in \mathbb{N}$ is some constant which depends on r , but not on m .

It is clear that this qubit string can be fed into the reference $UQTM\mathfrak{A}$ together with a description of the algorithm \mathfrak{A} of fixed length c' which depends on r , but not on m . This will give a qubit string $\sigma_{\mathfrak{A}}(\tilde{q})$ of length

$$\begin{aligned} \ell(\sigma_{\mathfrak{A}}(\tilde{q})) &= 2\lfloor \log m \rfloor + 2 + c + \lceil mr \rceil + c' \\ &\leq 2\log m + m \left(s + \frac{1}{2}\delta \right) + c'', \end{aligned} \quad (45)$$

where c'' is again a constant which depends on r , but not on m . Recall the matrix U constructed in step 11 of our algorithm \mathfrak{A} , which rotates (decompresses) a compressed (short) qubit string \tilde{q} back into the typical subspace. Conversely, for every one-dimensional projector $q \leq q_m$, where $q_m = Q_{s,\varepsilon}^{(m)}$ was defined in (40), let $\tilde{q} \in \mathcal{H}_{\lceil mr \rceil}$ be the projector given by $(|0\rangle\langle 0|)^{\otimes (m - \lceil mr \rceil)} \otimes \tilde{q} = U^* q U$. Then, since \mathfrak{A} has been constructed such that

$$\|\mathfrak{A}(\sigma_{\mathfrak{A}}(\tilde{q}), k) - q\|_{\text{Tr}} < \frac{1}{k} \quad \text{for every } k \in \mathbb{N},$$

it follows from (45) that

$$\frac{1}{m} QC^{\searrow 0}(q) \leq 2 \frac{\log m}{m} + s + \frac{1}{2}\delta + \frac{c''}{m}.$$

If m is large enough, Equation (24) follows.

Now we continue by proving Equation (25). Let $k := \lceil \frac{1}{2\delta} \rceil$. Then, we have for every one-dimensional projector $q \leq q_m$ and m large enough

$$\begin{aligned} \frac{1}{m} QC^{2\delta}(q) &\leq \frac{1}{m} QC^{1/k}(q) \leq \frac{1}{m} QC^{\searrow 0}(q) + \frac{2\lfloor \log k \rfloor + 2}{m} \\ &< s + \delta + \frac{2\log k + 2}{m} < s + 2\delta, \end{aligned} \quad (46)$$

where the first inequality follows from the obvious monotonicity property $\delta \geq \varepsilon \Rightarrow QC^{\delta} \leq QC^{\varepsilon}$, the second one is by Lemma 2, and the third estimate is due to Equation (24). \square

Proof of the Main Theorem 1. Let $\tilde{q}_m(\delta)$ be the Ψ -typical projector sequence given in Proposition 1, i.e. the complexities $\frac{1}{m}QC^{\setminus 0}$ and $\frac{1}{m}QC^\delta$ of every one-dimensional projector $q \leq \tilde{q}_m(\delta)$ are upper bounded by $s + \delta$. Due to Corollary 1, there exists another sequence of Ψ -typical projectors $p_m(\delta) \leq \tilde{q}_m(\delta)$ such that additionally, $\frac{1}{m}QC^\delta(q) > s - \delta(2 + \delta)s$ is satisfied for $q \leq p_m(\delta)$. From Corollary 2, we can further deduce that there is another sequence of Ψ -typical projectors $q_m(\delta) \leq p_m(\delta)$ such that also $\frac{1}{m}QC^{\setminus 0}(q) > s - \delta$ holds. Finally, the optimality assertion is a direct consequence of the Quantum Counting Argument, Lemma 3, combined with Theorem 2. \square

6. Summary and Perspectives

Classical algorithmic complexity theory as initiated by Kolmogorov, Chaitin and Solomonoff aimed at giving firm mathematical ground to the intuitive notion of randomness. The idea is that random objects cannot have short descriptions. Such an approach is on the one hand equivalent to Martin-Löf's which is based on the notion of *typicalness* [39], and is on the other hand intimately connected with the notion of entropy. The latter relation is best exemplified in the case of longer and longer strings: by taking the ratio of the complexity with respect to the number of bits, one gets a *complexity per symbol* which a theorem of Brudno shows to be equal to the *entropy per symbol* of almost all sequences emitted by ergodic sources.

The fast development of quantum information and computation, with the formalization of the concept of *UQTMs*, quite naturally brought with itself the need of extending the notion of algorithmic complexity to the quantum setting. Within such a broader context, the ultimate goal is again a mathematical theory of the randomness of quantum objects. There are two possible algorithmic descriptions of qubit strings: either by means of bit-programs or of qubit-programs. In this work, we have considered a qubit-based *quantum algorithmic complexity*, namely constructed in terms of quantum descriptions of quantum objects.

The main result of this paper is an extension of Brudno's theorem to the quantum setting, though in a slightly weaker form which is due to the absence of a natural concatenation of qubits. The quantum Brudno's relation proved in this paper is not a pointwise relation as in the classical case, rather a kind of convergence in probability which connects the *quantum complexity per qubit* with the von Neumann entropy rate of quantum ergodic sources. Possible strengthening of this relation following the strategy which permits the formulation of a quantum Breiman theorem starting from the quantum Shannon-McMillan noiseless coding theorem [8] will be the matter of future investigations.

In order to assert that this choice of quantum complexity as a formalization of "quantum randomness" is as good as its classical counterpart in relation to "classical randomness", one ought to compare it with the other proposals that have been put forward: not only with the quantum complexity based on classical descriptions of quantum objects [40], but also with the one based on the notion of *universal density matrices* [15].

In relation to Vitanyi's approach, the comparison essentially boils down to understanding whether a classical description of qubit strings requires more classical bits than s qubits per Hilbert space dimension. An indication that this is likely to be the case may be related to the existence of entangled states.

In relation to Gacs' approach, the clue is provided by the possible formulation of "quantum Martin-Löf" tests in terms of measurement processes projecting onto low-probability subspaces, the quantum counterparts of classical untypical sets.

One cannot however expect classical-like equivalences among the various definitions. It is indeed a likely consequence of the very structure of quantum theory that a same classical notion may be extended in different inequivalent ways, all of them reflecting a specific aspect of that structure. This fact is most clearly seen in the case of quantum dynamical entropies (compare for instance [3]) where one definition can capture dynamical features which are precluded to another. Therefore, it is possible that there may exist different, equally suitable notions of "quantum randomness", each one of them reflecting a different facet of it.

Acknowledgements. We would like to thank our colleagues Ruedi Seiler and Igor Bjelaković for their constant encouragement and for helpful discussions and suggestions.

This work was supported by the DFG via the project "Entropie, Geometrie und Kodierung großer Quanten-Informationssysteme" and the DFG-Forschergruppe "Stochastische Analysis und große Abweichungen" at the University of Bielefeld.

References

1. L.M. Adleman, J. Demarrais and M. A. Huang, "Quantum Computability", *SIAM J. Comput.* **26** 1524-1540 (1997)
2. V.M. Alekseev, M.V. Yakobson, "Symbolic Dynamics and Hyperbolic Dynamic Systems", *Phys. Rep.* **75** 287 (1981).
3. R. Alicki and H. Narnhofer, "Comparison of dynamical entropies for the noncommutative shifts", *Lett. Math. Phys.* **33** 241-247 (1995)
4. E. Bernstein, U. Vazirani, "Quantum Complexity Theory", *SIAM Journal on Computing* **26** 1411-1473 (1997)
5. A. Berthiaume, W. Van Dam and S. Laplante, "Quantum Kolmogorov complexity", *J. Comput. System Sci.* **63** 201-221 (2001)
6. P. Billingsley, "Ergodic Theory and Information", *Wiley Series in Probability and Mathematical Statistics*, John Wiley & Sons, New York 1965
7. I. Bjelaković, T. Krüger, Ra. Siegmund-Schultze, A. Szkola, "The Shannon- McMillan theorem for ergodic quantum lattice systems", *Invent. Math.* **155** 203-222 (2004)
8. I. Bjelaković, T. Krüger, Ra. Siegmund-Schultze and A. Szkola, "Chained Typical Subspaces- a Quantum Version of Breiman's Theorem", *quant-ph/0301177*
9. I. Bjelaković and A. Szkola, "The Data Compression Theorem for Ergodic Quantum Information Sources", *Quant. Inform. Proc.* **4** No. 1 49-63 (2005)
10. A. A. Brudno, "Entropy and the complexity of the trajectories of a dynamical system", *Trans. Moscow Math. Soc.* **2** 127-151 (1983)
11. G. J. Chaitin, "On the Length of Programs for Computing Binary Sequences", *J. Assoc. Comp. Mach.* **13** 547-569 (1966)
12. T. M. Cover, J. A. Thomas, "Elements of Information Theory", *Wiley Series in Telecommunications*, John Wiley & Sons, New York 1991
13. D. Deutsch, Quantum theory, the Church-Turing principle and the universal quantum computer, *Proc. R. Soc. Lond.*, **A400** (1985)
14. R. Feynman, Simulating physics with computers, *International Journal of Theoretical Physics*, **21**(1982) pp. 467-488
15. P. Gács, "Quantum algorithmic entropy", *J. Phys. A: Math. Gen.* **34** 6859-6880 (2001)
16. J. Gruska, "Quantum Computing", *McGraw-Hill, London* 1999
17. F. Hiai, D. Petz, "The Proper Formula for Relative Entropy and its Asymptotics in Quantum Probability", *Commun. Math. Phys.* **143** 99-114 (1991)
18. A. S. Holevo, "Statistical Structure of Quantum Theory", *Springer Lecture Notes* **67** (2001)
19. R. Jozsa and B. Schumacher, "A new proof of the quantum noiseless coding theorem", *J. Mod. Optics* **41** 2343-2349 (1994)

20. R. Jozsa, M. Horodecki, P. Horodecki and R. Horodecki, "Universal Quantum Information Compression" *Phys. Rev. Lett.* **81** 1714-1717 (1998)
21. A. Kaltchenko and E. H. Yang, "Universal compression of ergodic quantum sources", *Quantum Information and Computation* **3**, No. 4 359-375 (2003)
22. G. Keller, "Wahrscheinlichkeitstheorie", *Lecture Notes, Universität Erlangen-Nürnberg* (2003)
23. J. Kieffer, "A unified approach to weak universal source coding", *IEEE Trans. Inform. Theory* **24** No. 6 674-682 (1978)
24. A. N. Kolmogorov, Three Approaches to the Quantitative Definition on Information, *Problems of Information Transmission* **1** 4-7 (1965)
25. A. N. Kolmogorov, "Logical Basis for Information Theory and Probability Theory", *IEEE Trans. Inform. Theory* **14**, 662-664 (1968)
26. M. Li and P. Vitányi, "An Introduction to Kolmogorov Complexity and Its Applications", *Springer Verlag* 1997
27. C. Mora and H. J. Briegel, "Algorithmic complexity of quantum states", [quant-ph/0412172](#)
28. C. Mora and H. J. Briegel, "Algorithmic complexity and entanglement of quantum states", [quant-ph/0505200](#)
29. M. A. Nielsen, I. L. Chuang, "Quantum Computation and Quantum Information", *Cambridge University Press, Cambridge*, 2000
30. M. Ozawa and H. Nishimura, "Local Transition Functions of Quantum Turing Machines", *Theoret. Informatics and Appl.* **34** (2000) 379-402
31. V. Paulsen, "Completely Bounded Maps and Operator Algebras", *Cambridge Studies in Advanced Mathematics* **78** (2002)
32. S. Perdrix, P. Jorrand, "Measurement-Based Quantum Turing Machines and their Universality", [quant-ph/0404146](#)
33. D. Petz and M. Mosonyi, "Stationary quantum source coding", *J. Math. Phys.* **42** 4857-4864 (2001)
34. P. Shor, "Algorithms for quantum computation: Discrete log and factoring", *Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science* (1994)
35. G. Segre, "Physical Complexity of Classical and Quantum Objects and Their Dynamical Evolution From an Information-Theoretic Viewpoint", *Int. J. Th. Phys.* **43** 1371-1395 (2004)
36. R. J. Solomonoff, "A Formal Theory of Inductive Inference", *Inform. Contr.* **7** 1-22, 224-254 (1964)
37. D. M. Sow, A. Eleftheriadis, "Complexity distortion theory", *IEEE Trans. Inform. Theory*, **IT-49**, 604-608 (2003)
38. K. Svozil, "Randomness and Undecidability in Physics", *World Scientific* (1993)
39. V.A. Uspenskii, A.L. Semenov and A.Kh. Shen, "Can an individual sequence of zeros and ones be random", *Uspekhi Mat. Nauk.* **45/1** 105-162 (1990)
40. P. Vitányi, "Quantum Kolmogorov complexity based on classical descriptions", *IEEE Trans. Inform. Theory* **47/6** 2464-2479 (2001)
41. H. White, "Algorithmic complexity of points in a dynamical system", *Erg. Th. Dyn. Sys.* **13** 807 (1993)
42. J. Ziv, "Coding of sources with unknown statistics-I: Probability of encoding error", *IEEE Trans. Inform. Theory* **18** 384-389 (1972)
43. A. K. Zvonkin, L. A. Levin, "The complexity of finite objects and the development of the concepts of information and randomness by means of the theory of algorithms", *Russian Mathematical Surveys* **25** No. 6 83-124 (1970)

Communicated by M. B. Ruskai